REVISITING CONTAINMENT STRATEGY IN THE DIGITAL AGE

Corneliu Bjola (University of Oxford)
James Pamment (Lund University)

Abstract: Since the Ukraine conflict began in 2014, there has been an increased awareness of the threat to EU interests posed by Russia. In early 2015, the EEAS created the East StratCom Team to respond by promoting the EU's soft power, strengthen media resilience, and catalogue disinformation. This article categorises several examples of Russian disinformation in order to conceptualise the conduct of digital warfare and suggest how it might be contained. We argue that Russian disinformation earns its effectiveness by focusing upon efforts to exploit differences between EU media systems (strategic asymmetry), the targeting of disenfranchised or vulnerable audiences (tactical flexibility), and the ability to mask the sources of disinformation (plausible deniability). We argue that the EU and NATO's response should be informed by a strategy of digital containment based on the tenets of supporting media literacy and source criticism, encouraging institutional resilience, and promoting a clear and coherent strategic narrative capable of containing the threat from inconsistent counter-messaging.

Keywords: European Union, Russia, Ukraine, NATO, disinformation, propaganda, digital containment

Bio notes:

Corneliu Bjola is Associate Professor in Diplomatic Studies at the University of Oxford. His research interests lie at the intersection of diplomatic studies, negotiation theory, international ethics, and crisis management. He has authored or edited five books, including the recent co-edited volumes *on Secret Diplomacy: Concepts, Contexts and Cases* (Routledge, 2015) and *Digital Diplomacy: Theory and Practice* (Routledge, 2015).

James Pamment is Senior Lecturer in Strategic Communication at Lund University, Sweden. His research interests lie at the intersection of strategic communication, diplomatic studies and international development. He is author of *British Public Diplomacy & Soft Power: Diplomatic Influence & Digital Disruption* (Palgrave, 2016) and *New Public Diplomacy in the 21st Century* (Routledge, 2013).

I. INTRODUCTION

The ambition of influencing “collective attitudes by the manipulation of significant symbols” or more simply put, by propaganda (Lasswell 1927, p. 627), has informed the thinking of political leaders, military strategists and diplomats for centuries. Machiavelli considered such forms of manipulation essential for maintaining the reputation and authority of the Prince (Machiavelli 2005, p. 62), von Clausewitz saw it as vital element in war that could motivate one’s troops and demoralise the enemy (Marlin 2002, p. 59), while George Kennan stressed the need for containing the “negative and destructive” Soviet propaganda with an “intelligent and really constructive program” (Kennan 1946, part 5). To be sure, the appeal of propaganda cannot be easily dismissed. It offers users a relatively cost-effective instrument for pursuing goals with presumably minimal resistance. If “soft power” is about attracting others to do what you want (Nye 2004, p. 5), then propaganda has to be understood as its “dark side”: attraction in the latter case is not the result of free choice, but of the amputation of choice. In other words, the audience is being compelled to make a choice out of a narrow set of options strategically defined by the propagandist, a practice known as “reflexive control” in Russia or “perception management” in the West (see more below).

As Kennan insightfully noted seven decades ago, the more negative and destructive the propaganda is, the more likely it is to collapse under its own weight, especially when it is confronted with a policy of “long-term, patient but firm and vigilant containment” (X 1947, p. 575). But what if the line between soft power and propaganda turns so thin that it becomes difficult to make sense of how much choice one is being denied? In Kennan’s time, the lines of propaganda were sharply drawn: one could be either on the side of Soviet communism or Western capitalism.[1] Nowadays, in the information rich environment of the digital age, disinformation is much more nuanced and hence more difficult to challenge and discredit. When information is abundant and easily accessible, its value depreciates. The cards are thus stacked against the constructive exchange of ideas and in favour of distorted and polarised communication. The numbers speak for themselves. Every minute of the day 347,222 tweets are sent out, 4,1666,667 Facebook likes are posted, 300 hours of new video are uploaded on YouTube, 1,736,111 photos on Instagram are liked, 1,041,666 Vine videos are played and so on (James, 2015). Given the sheer magnitude of the global production and consumption of digital data, states face serious challenges to monitor, let along effectively confront the sources of propaganda leveraged against them.

The ongoing campaign of disinformation (see EU definition of the term further below) conducted by Russia in Western and especially Eastern Europe fits well within this description. It is not as blatantly provocative as the Soviet propaganda during the Cold War, nor does it follow the transparent prescriptions of soft power norms. It has instead adopted a fluid approach to ideology that allows the Kremlin to simultaneously back far-left and far-right movements, greens, anti-globalists and financial elites with the aim to exacerbate divides in the West and to create an echo chamber of Kremlin support (Pomerantsev and

[1] While Kennan stopped short from explicitly endorsing the use of propaganda in his Long Telegram, his containment strategy left the door open for such engagements. Countering the Soviet threat, in his view, would require the coordination of of political and military strategy, domestic and foreign policy in a manner comparable with wartime strategy (Defty 2013: 37).

Weiss 2014, p. 6). Most importantly, it works, to the extent that some of Kremlin's authoritarian policies have become a point of reference and even admiration for a number of European political leaders and policy-makers (The Economist, 2015; Orenstein, 2014).

In this article, we focus on the digital dimension of the Russian campaign of disinformation in Europe, describe its mode of operation, and discuss its viability as an instrument of digital warfare. Echoing Kennan, we conclude that the Russian digital propaganda strategy can be successfully confronted with a policy of firm digital containment, designed to confront the Kremlin with digital counter-force at every point where it shows signs of encroaching upon the interests and stability of the West. We develop this argument in four steps. First, we draw on the work of the recently established East StratCom Team to contextualise the state of play of Russian digital propaganda in Europe. Second, we elaborate on four patterns by which Russia conducts its campaign of digital disinformation. Third, we investigate the strengths and limitations of the Russian propaganda as an instrument of digital warfare. Fourth, we discuss the key components of the digital containment strategy that could undermine Russian efforts to weaponise information against the West.

II. EUROPE'S COUNTER-DISINFORMATION STRATEGY

Since the Ukraine conflict began in early 2014, the European Union has struggled to find a means of countering Russian influence over the circulation of information about geopolitical issues in its eastern regions and the eastern neighbourhood. An initiative proposed by Lithuania, the UK, Denmark and Estonia called for "credible and competitive information alternatives for Russian-speaking populations and those using Russia's state-controlled media" (BNS, 2015). This was raised at the European Council in March 2015, and the EC duly "stressed the need to challenge Russia's ongoing disinformation campaigns" in Europe (European Council, 2015).

Consequently, a small strategic communications group called the East StratCom Team was established by the European External Action Service (EEAS) to coordinate member states and EU institutions in the development of a formal action plan to combat Russian influence. Its mission is not simply to counteract Russia's disinformation surrounding the conflict in Ukraine, but also to strengthen "wider EU efforts in support of media freedom and strengthening of the overall media environment" (East StratCom Team 2015). In other words, this advance in the EU's strategic communication capacity is not simply limited to counteracting specific disinformation, but also to promoting structural changes to the media environment in a manner that reinforces the influence of the EU and its values. Consolidating the EU's soft power capacity is an inherent part of this strategy. These goals were narrowed down into three strands in its June 2015 action plan:

1. Effective communication and promotion of EU policies and values towards the Eastern neighbourhood;
2. Strengthening of the overall media environment in the Eastern Neighbourhood and in EU Member States;

3. Improved EU capacity to forecast, address and respond to disinformation activities by external actors (East StratCom Team, 2015).

The action plan is multifaceted and aims to strengthen EU strategic communication through a number of parallel initiatives. These include the creation of persuasive messaging, the development of civil society networks, facilitating targeted support via EU funded programmes, journalist support and capacity building, public diplomacy initiatives, and strengthened cooperation on regulatory issues. Perhaps most notably, the guiding principle of the initiative is to "allow citizens to easily understand that political and economic reforms promoted by the EU can, over time, have a positive impact on their daily lives" (East StratCom Team 2015, p. 1). There is therefore a clear ideological dimension to countering Russian influence; the goal is to contain the threat by developing resilience through the soft power of values and ideals.

Its target countries include Armenia, Azerbaijan, Belarus, Georgia, Moldova, Russia and Ukraine, along with EU countries with Russian-speaking minorities. Achievements during 2015 include the launch of a Russian language Twitter feed (@eu_eeas) and other social media content, the development of a "campaigning approach" to promotion of EU policies in target countries, and the creation of a Russian Language News Exchange and Baltic Media Centre of Excellence (EEAS, 2015). In addition, a number of national broadcasters, most notably the BBC and Deutsche Welle, have undertaken to launch Russian-language news channels.

With regards to disinformation, the action plan aims to contain Russian influence through activities that "develop critical thinking and promote media literacy" (East StratCom Team 2015, p. 3). This includes "finding, documenting and promoting best practice in the field of media literacy" (East StratCom Team 2015, p. 3). One of the main products is the Disinformation Review, launched in October 2015, to provide a weekly compilation of Russian-sourced stories planted in European media. The Disinformation Review takes the form of a spreadsheet which captures the date, language/target audience, a summary of the disinformation, a link to the story, links to its disproof, and the name of the group who found the disinformation. A network of journalists and NGOs collect the sources, which are compiled by East StratCom. An associated @EUvsdisinfo Twitter account was also created. The objectives of the Disinformation Review initiative are:

> to show the European public the high amount of such disinformation attacks that target European audience[s] every single day, to expose the number of countries targeted, and, thus, to explain to the European audience the breadth of this problem. The data and information collected would help to conduct a better analysis and, thus, be ready to counter and pre-empt possible misinformation attacks in the future (Delegation of the European Union to Ukraine, 2015).

Parallel to the "recent security-related developments" that necessitated these new policies, the European Parliament released an up-to-date series of definitions of certain key terms surrounding the manipulation of media (EPRS 2015). This defined *disinformation* as "systematic and intentional deception" by manipulating the flow of information in a manner that can adversely affect the values of a society. *Misinformation* was defined as "unintentionally incorrect information," on the basis that such factually incorrect information is not deliberately designed to mislead. The paper also notes that the European Parliament has interchangeably referred to Russian information activities as *disinformation*, *misinformation* and *political propaganda* (as may also be observed in the above quote from the EU Delegation to Ukraine), but that East StratCom's Disinformation Review is explicit in characterising the collected data as intending to deceive (EPRS 2015, p. 2).[2]

Some methodological strengths and limitations in the Disinformation Review may be observed. Most problematic is the distributed nature of the so-called EU Mythbusters network. On the one hand, it offers a breadth of language skills and local media knowledge that enables the collection of data from across Europe and the Eastern neighbourhood. However, the informal nature of network membership means that some countries are better covered than others, some are only covered for short periods, and that the interests of the reporting organisations may skew the kinds of information reported. Thus, the weekly compilations represent a somewhat inconsistent sample of Russian disinformation. RT was quick to go on the offensive, comparing Mythbusters to the movie Ghostbusters, and offering a comprehensive rebuttal of the scheme. This included accusing the West of ganging up on Russia, of holding Russian media to different standards than Western media, and of exaggerating Russian expenditure on international communications. Furthermore, RT sought to discredit the individuals involved in the initiative.

> Despite their abundance of resources, the Western establishment is constantly scheming up new ways to reverse the supposed 'infowar' losses to Russia. Yet with every new "strategic communication" effort, it becomes apparent that EU's, and the West's messaging problem is neither money nor shortage of special ~~ghostbusters~~ mythbusters initiatives but the trite, tired, and Cold War-mired narratives that are still been served to their viewers, readers and listeners (RT, 2015).

We consider certain aspects of the Disinformation Review to be problematic. For example, it is not possible to ascertain whether a certain story is disinformation or misinformation before the data has been assessed, and hence it appears presumptive to categorise all collected data as disinformation. Furthermore, the collection process is highly politicised, both in the membership of the Mythbusters network, and in the overall objectives of East StratCom's mandate. While this suggests that the Disinformation Review is a contentious project, it nonetheless provides an important platform for collecting raw data that may otherwise be unavailable to policymakers and researchers. With these caveats in mind, we approach the Disinformation Review as a potentially valuable source of empirical data for better understanding the nature of the present digital information war in Europe.

III. PATTERNS OF DISINFORMATION

[2] "Deliberately misleading" is quite difficult to ascertain empirically since the actors involved in this practice may sincerely believe in what they argue for, including conspiracy theories. However, this is an assumption in the EEAS' process of collecting data, and hence underpins their interpretation of how their opponent works.

Following the first 10 weeks of Disinformation Reviews, we conducted an initial analysis of the data in order to determine the most common basic forms of disinformation captured by East Stratcom's sources. This method is known is "qualitative thematic analysis," and involves grouping a source material based upon shared themes or qualities. This is done with the aim of determining a number of overarching categories which can be used to group present as well as future data (Silverman, 2006). We determined four basic categories of disinformation based on the data:

- Unsourced or falsified claims
- Non-credible claims with sources
- Claims based on earlier unsourced or non-credible claims
- Conspiracy theories

The examples given below are for the purpose of elucidating these categories, and are all taken from the Disinformation Review published on 17 November 2015.

- *Unsourced or falsified claims:* unsourced or falsified claims are those that seek to mislead deliberately. They tend to circulate false information by lying, obscuring the source or by presenting assertions as facts. A common theme throughout the Disinformation Reviews is stories about the Crimea conflict that fit within a traditional propaganda model. For example, news stories aimed at Russian and Ukrainian audiences claimed that the Ukraine was arming ISIL via an American military base in Turkey, though no evidence was presented and the story was attributed "according to news sources" (Economics & We, 2015). Similar unsourced stories claim that Canadian mercenaries have joined the Ukrainian army, and that the Ukrainian army shelled civilians in Orlovka (Sputnikbig.ru, 2015). This category therefore represents the most straightforward examples of disinformation.

- *Non-credible claims with sources:* non-credible claims are those which have a genuine source (usually within the political or scientific communities), but whose claims are treated uncritically. For example, an article on the Swedish and Norwegian language *Sputnik* websites claims that the European Commission gave Serbia a low score in its ratings of EU candidate countries because of its close relations with Russia (Sputnik 2015a, 2015b). The article is based upon a statement by Serbian Prime Minister Aleksandar Vučić, which itself responds to approximately two paragraphs out of the 80-page review by the EC. These paragraphs centre on the critique that Serbia has not aligned itself with EU decisions on Crimea, Bosnia and Herzegovina and Moldova (European Commission 2015, p. 70). The Sputnik article reports these statements without giving any of the wider context or background to how the European Commission makes its assessments, thereby shifting attention away from the repeat allegations of high-level corruption in Serbia detailed in the report. This category is more problematic because it is based upon the opinions of people with credible positions, but acts as disinformation because those opinions are framed in an unbalanced or uncritical manner that is intended to mislead.

- *Claims using earlier unsourced or non-credible claims as a source:* this category builds on the two approaches referred to above by using similar stories published in the past as the sources for new claims. It refers, in other words, to stories that use previous disinformation as a source of credibility. For example, a story published in the Czech Free Press (2015) claims that Germany and the EU want to legalise paedophilia. The Mythbusters network member reporting the story notes that such stories have been circulated since 2009, but that the source document referred to in earlier stories does not exist. Hence, this story deliberately misleads by echoing previous disinformation.

- *Conspiracy theories:* the final category is conspiracy theories, or disinformation that claims to reveal some form of truth that the mainstream media will not. For example, a 23-minute English-language Youtube video posted by *Russia Insider* claims to be a "Bombshell video" with "Vital Litvinenko Murder Clues Unearthed by Amateur Sherlock Fans".[3] Its presenter is introduced as the "Russian Sherlock Holmes" and explains that the purpose of the video is to discover the truth of the case through scientific rather than political reasoning in order to improve relations between Britain and Russia. It includes a polygraph test with Andrej Lugovoy, one of the main suspects in the murder. Evidence presented in the video suggests that Litvinenko was poisoned at a different restaurant to the one proposed by the British investigators, but that this has been ignored because it does not suit Britain's political agenda. The purpose of the video seems to be to add a layer of doubt to the 'official' narrative and make allusions to a deeper conspiracy surrounding the investigation. Such approaches use doubt and a mistrust of power to undermine other countries or actors.

While these categories are not exhaustive, they offer some shape to the disinformation strategies that Europe and the Eastern Neighbourhood currently face.

IV. CONCEPTUALISING DIGITAL WARFARE

The evidence collected thus far by the East StratCom Team supports the view, in rather strong terms, that such methods of disinformation are part of a deliberate strategy, which we hereby refer to as digital warfare. Similar to the concept of "hybrid warfare" which covers "asymmetric battlegrounds within the conflict zone population, the home front population, and the international community population" (Mccuen, 2008, p. 107), digital warfare aims to increase one's strategic advantage over opponents, but with a narrower focus on information manipulation in the digital sphere. To be sure, information operations have been long recognised by all major powers as key components of military strategy (Ventre, 2011), but what digital warfare brings to the table is the strategic use of IT tools and social media networks to intimidate, undermine and ultimately defeat an opponent short of military action In brief, digital warfare builds on traditional concepts of coercive diplomacy (George 1991) and compellence (Schelling 1966) and involves the weaponisation of information in the digital sphere and is characterised by the following core features:

[3] https://www.youtube.com/watch?v=2Xq3LXKnatw

- *Strategic asymmetry*: this refers to the use of non-military means to achieve political and strategic goals. Asymmetry in this case follows not from engaging in unconventional tactics to compensate for deficient military power and resources, as in classical situations of guerrilla warfare (Joes, 1996), but from applying unconventional tactics to pursue political goals that are more difficult or costly to achieve by military means. Asymmetrical tactics include, for instance, systematic abuse of democratic media structures in the West by means of misleading and biased articles (Jackson, 2015) or divide and rule strategies exploiting weaknesses in the European political system or decision-making with the aim to unpick the fabric of European unity on a whole range of vital strategic issues (Foster and Holehouse, 2016). They are particularly characterised by the low economic and political costs to the sender of this information, and to the low levels of investment in the success or failure of any individual propaganda messages. As the Ukraine case suggests, military means may follow in case asymmetrical tactics fail to deliver, but the cost effective preference is to pressure the opponent to "voluntarily" pursue goals in line with one's agenda. [4]

- *Tactical flexibility*: the strategic objective of digital warfare is to achieve "reflexive control", which refers to the method "of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action" (Thomas, 2004, p. 237). However, from a tactical perspective, the key aspect of the theory is the "reflex" part, which "involves the specific process of imitating the enemy's reasoning or imitating the enemy's possible behaviour and causes him to make a decision unfavourable to himself" (Thomas, 2004, p. 241). In other words, in order for digital warfare to be successful and achieve reflexive control, it needs to be tailored to the specific profile of the target audience, as some of the examples presented in the previous section illustrate, such as the story about "Russian Sherlock Holmes" tailored to the UK audience or the distorted interpretation regarding of the EC report on Serbia planted in the Norwegian media. Of particular importance here is the vulnerability of specific audience groups due to their disenfranchisement from mainstream media, or lack of access to balanced information sources.

- *Plausible deniability* – The ability to mask one's digital identity or to decline responsibility for actions involving deliberate deception or disinformation could be a valuable asset when engaging in digital warfare. The inherent nature of cyberspace allows users to operate with a high degree of anonymity, as Internet activity can be routed through numerous Internet service providers (ISPs) or "botnets" (i.e. compromised computers controlled by an unknown third party). This way, states accused of digital warfare may simply ignore, deny or shift the blame to non- state actors without fear of serious consequence (Coward and Bjola, 2016, p. 207).

[4] The cost of the Russian intervention in Ukraine has been estimated, for instance, to have risen to 53 billion rubles (approx. 0.7 billion USD) in the first ten months of the conflict in eastern Ukraine, not including the 80 billion rubles allocated for supporting "refugees" from the Donetsk and Luhansk regions in eastern Ukraine (Dolgov 2015). By contrast, the budget of Russia Today (RT), the main outlet of the Russian propaganda machine amounted to about 15.4 billion rubles ($240 million) in 2015 (Bershidsky 2015a).

> Plausible deniability presents thus the dual advantage of keeping opponents off-balance with regards to one's strategical goals and of enhancing the credibility of the message via third parties such as sympathetic digital proxies of remotely controlled local websites (Kennedy and Kralova, 2015).

While digital warfare may impress by its technological novelty and cost-effectiveness, one should be careful not to overstate its capacity to deliver results. Strategic asymmetry may not actually pay off when important values are at stake. The strategy of sending out multiple, often contradictory messages does not suggest a coherent strategy capable of leading to a defined outcome, so much as haphazard efforts at destabilisation. Russia actually had to intervene military in Ukraine to accomplish its goals as most Ukrainians opposed Moscow's agenda in the country (Snegovaya 2015, p. 19). The impact of Russian propaganda in the West also remains limited despite the significant resources spent on improving Russian "soft power". President Putin's negative ratings often exceed 75 percent in various part of the world, including Europe where they reach the unenviable level of 85% (Bershidsky, 2015b), However, as mentioned above, he remains popular with some European political leaders and policy-makers, especially on the populist right side of the spectrum. Tactical flexibility is critical for contextualising the message, but it may prompt coordination issues regarding the various components of the overall strategic agenda and may invite misleading parallels about the impact of digital warfare in different regions (e.g., Russian involvement in Ukraine my predict similar interventions in the Baltic region or elsewhere despite important contextual differences) (Charap, 2015). Finally, plausible deniability may work in the short term, but it may have exactly the opposite effect in the longer term as Russian disinformation may be suspected by Western audiences to transpire even when that might not be the case (Galeotti, 2015).

V. MAKING DIGITAL CONTAINMENT WORK

While the short term impact of Russian digital propaganda in the West may be rather difficult to reliably assess, its long-term impact is too risky to ignore. Long term exposure to digital trolling has been shown, for instance, to reshape personal values and beliefs even when people initially demonstrated strong resistance to the propaganda message (Spruds et al. 2015, p. 81). The matter thus needs to be taken seriously, but handled with care. NATO is considering, for instance, developing its own form of strategic communication as a counterbalance to the Russian campaign of disinformation, but the scope of the strategy is a subject of debate. Some key members worry that by copying Russian methods the credibility of the organisation might suffer serious damage. As the NATO spokesperson points out "one of the main principles of NATO is that we cannot counter propaganda with more propaganda" (Emmott, 2016). One alternative that NATO may consider adopting, and which we are keen to advocate here, is that NATO should resist the temptation of joining the "dark side" of propaganda and instead embrace a strategy of digital containment, designed to confront Kremlin with digital counter-force at selective critical points where it shows signs of encroaching upon the interests and stability of the West.

While the Cold War containment strategy was designed to confront a different type of threat that is, communism expansion (Gaddis, 2005), its core principle of resisting conventional threats to the West with comparable "counterforce" retains conceptually valid for confronting digital warfare as well, on three grounds. First, it offers a "cold" instrument for curtailing Russian ambitions in Europe short of open military conflict. While the risk of military confrontation between Russia and the West remains low, digital containment could help prevent military escalations especially in those regions in Eastern Europe that are more vulnerable to "hybrid" interventions. Second, it can rebuild confidence in European institutions by demonstrating their resilience. The asymmetrical tactics used by Russia against the West have exposed a series of digital weaknesses and "blind spots" in European institutions which must be properly addressed if they are to function properly and to survive. Third, digital containment may also serve as a deterrent against further digital incursions against the West. Digital warfare works as long as its benefits are perceived to offset the costs, but if the latter can be increased by a strategy of digital containment then the incentive for engaging in such activities will proportionally decline.

The digital containment strategy we propose takes note of the three elements of digital warfare discussed in the previous section and seeks to blunt their effectiveness by closing the strategic asymmetry gap, obstructing tactical flexibility and by denying deniability. As a first step, the opportunities that allow Russian information strategists to asymmetrically exploit weaknesses in the European digital sphere must be closed off. This would imply, for instance, that main outlets of Russian disinformation such as RT[5] or Sputnik should be more closely scrutinised by the relevant regulatory agencies for their compliance with European codes of journalism standards. Work is currently under way for improving the European regulatory environment and for enhancing collaboration between national regulators, including through meetings of the European Regulators Group (Rettman, 2015), but these efforts must be accelerated, streamlined and targeted to digital platforms. This is important because RT and Sputnik provide the information resources and create the echo-chambers by which disinformation is being disseminated and reinforced online by sympathetic or Russian controlled websites and social media accounts. Unlike the situation in Russia, where severe restrictions have been enacted against social media users who voice criticism against the regime (BBC, 2014), EU countries cannot blacklist or suspend Russian propaganda websites or social media accounts as that would contravene the democratic norms they have fought hard to defend. They can nevertheless selectively focus on the most influential online nodes of propaganda dissemination and deploy "digital debunking" teams to professionally query the authors for the source of their stories and to carefully correct misleading or false statements. This way they can deprive these nodes of an important communicational advantage (i.e., promoting one-sided views without challenge), increase the costs of the other side for sustaining their message and disrupt the communication lines that sustain the Russian echo-chambers of bias confirmation against the West.

As pointed out above, tactical flexibility allows disinformation operators to adjust the message to the local audience while still following the same strategic direction. A recent report has revealed, for instance, that Sputnik's modus operandi of reporting in Central and

[5] While RT is a TV news channel, it has a digitized format i.e., it is broadcast digitally by satellite and internet. Digital convergence thus makes difficult to make strong delimitations between mainstream and online media.

East European countries is to select a small number of anti-establishment politicians and give them substantial coverage, while reporting little or nothing about the representatives of other parties or points of view (Nimmo 2016, p. 3). In line with the prescriptions of the "reflexive control" theory, the desired effect of tactical contextualisation is the creation of a manufactured impression of growing online opposition to policies not aligned with the Russian strategic agenda in the region. The way this tactic could be rendered ineffectual is by inducing "frame breaking", which in Goffman's parlance refers to the acts by which a performer fails to sustain the script he has been asked to follow (Goffman 1975, p. 216) . In other words, "performers" should be hindered in their efforts to anchor digital frames of disinformation to the local context. They should be also drawn into frame disputes that would make more difficult for them to follow the original script. Social network analysis could help, for instance, to identify digital gatekeepers of the information flow (Bjola, 2016) who need to be isolated online in order for the local anchoring of disinformation to break. In addition, sustained efforts should be made to take the initiative in the digital sphere and promote a robust strategic narrative that would make it more difficult for digital propagandists to respond without contradicting themselves (Miskimmon et al, 2015).

Finally, denying plausible deniability to digital disinformation advocates is a critical step for the success of the digital containment strategy. As long as disinformation can be disseminated with impunity, the promoted message retains a certain degree of credibility, especially when it is associated with a local account. While revealing the identity of online users involved in disinformation campaigns often remains a technical challenge and a politically sensitive issue, pattern recognition using qualitative and data visualisation techniques could prove more effective and arguably less controversial as an instrument of digital identification. The four patterns of disinformation presented above offer a good starting point for localising sources of Russian digital warfare. The key point of this approach is not that it can unequivocally reveal a "smoking gun" of Russian government involvement and coordination of digital disinformation activities in Europe, but rather that it can empower users of digital media to understand what kinds of information they are consuming. Data visualisation techniques such cluster analysis, diffusion mapping or anomaly detection (Pitas, 2015) can provide further confirmation of the extent to which similar messages of digital disinformation are disseminated, from which sources, and with what degree of confidence. The data so collected could then be fed back into "frame breaking" methods and periodically reported to the public in an effort to increase societal resilience to further disinformation campaigns.

In conclusion, the establishment of the East StratCom Team is a good start for countering the systematic disinformation campaign launched by Russia against the West. In order to be effective, substantial resources needs to be deployed behind a clear strategy of digital containment aimed at closing the strategic asymmetry gap, obstructing tactical flexibility and denying the plausible deniability of disinformation operators. The EU and NATO's strategy should be based on the tenets of supporting media literacy and source criticism, encouraging institutional resilience, and promoting a clear and coherent strategic narrative capable of containing the threat from inconsistent counter-messaging. Ultimately, the citizens of the EU and Eastern neighbourhood must be supported so that they can cease to be targets of propaganda, and instead act as nodes in its containment.

REFERENCES:

BBC. 2014. "Russia enacts 'draconian' law for bloggers and online media." BBC, Last Modified Aug 1 Accessed Feb 16. http://www.bbc.co.uk/news/technology-28583669.

Bershidsky, Leonid. 2015a. "Putin's Propaganda Industry Tightens Its Belt." BloombergView, Last Modified Jan 23 Accessed Feb 5. http://www.bloombergview.com/articles/2015-01-23/putin-s-propaganda-industry-tightens-its-belt.

Bershidsky, Leonid. 2015b. "Why world still hates Russia despite $500m propaganda spend." Bloomberg, Last Modified Aug 6 Accessed Feb 8. http://www.biznews.com/leadership/2015/08/06/bloomberg-view-why-world-still-hates-russia-despite-500m-propaganda-spend/.

Bjola, Corneliu. 2016. "Is Resistance Futile? Maximizing the Impact of Public Diplomacy on Social Media." USC Center on Public Diplomacy, Last Modified Jan 15 Accessed Feb 17. http://uscpublicdiplomacy.org/blog/resistance-futile-maximizing-impact-public-diplomacy-social-media.

BNS (2015) "Lithuania, UK, Denmark and Estonia call for EU plan against Russian propaganda," Delfi (9 January 2015). Retrieved from http://en.delfi.lt/eu/lithuania-uk-denmark-and-estonia-call-for-eu-plan-against-russian-propaganda.d?id=66857976

Charap, Samuel. 2015. "The Ghost of Hybrid War." *Survival* 57 (6):51-58. doi: 10.1080/00396338.2015.1116147.

Coward, Ashley, and Corneliu Bjola. 2016. "Cyber-Intelligence and Diplomacy: The Secret Link." In *Secret diplomacy : concepts, contexts and cases*, edited by Corneliu Bjola and Stuart Murray, 201-228. Abingdon, Oxon ; New York, NY: Routledge.

Czech Free Press! (2015) 'Germany and the EU want to legalize pedophilia'. http://www.czechfreepress.cz/evropa/nemecko-a-eu-chteji-legalizovat-pedofilii.html

Defty, A. 2013. *Britain, America and Anti-Communist Propaganda 1945-53: The Information Research Department*. Abingdon, Oxon ; New York, NY: Routledge.

Delegation of the European Union to Ukraine (2015) "Disinformation Review" - new EU information product (04/11/2015). Retrieved from http://eeas.europa.eu/delegations/ukraine/press_corner/all_news/news/2015/2016_11_04_1_en.htm

Dolgov, Anna. 2015. "Nemtsov Report Details Human and Financial Costs of War in Ukraine." Moscow Times, Last Modified May 12 Accessed Feb 5. http://www.themoscowtimes.com/news/article/nemtsov-report-details-human-and-financial-costs-of-war-in-ukraine/520571.html.

East StratCom Team (2015) Action Plan on Strategic Communication (Ref. Ares(2015)2608242 - 22/06/2015). Retrieved from http://eap-csf.eu/assets/files/Action%20PLan.pdf

Economics & We (2015) 'Ukraine Equips ISIL!'. http://economicsandwe.com/F01A5181270F6F4E/

EEAS (2015) EU East Stratcom Task Force (November 2015). Powerpoint.

European Council (2015) European Council Conclusions on external relations (19 March 2015). Press release 134/15. Retrieved from http://www.consilium.europa.eu/en/meetings/european-council/2015/03/19-20/

European Commission (2015) Serbia 2015 Report (SWD(2015) 211 final). Brussels: European Commission

EPRS (European Parliamentary Research Service) (2015) At a glance: Understanding propaganda and disinformation (November 2015). PE 571.332

Emmott, Robin. 2016. "NATO may start using military tactics to try and combat Russian propaganda." Reuters, Last Modified Jan 27 Accessed Feb 8. http://uk.businessinsider.com/r-nato-looks-to-combat-russias-information-weapon-document-2016-1?r=US&IR=T.

Foster, Peter, and Matthew Holehouse. 2016. "Russia accused of clandestine funding of European parties as US conducts major review of Vladimir Putin's strategy." The Telegraph, Last Modified Jan 16 Accessed Feb 15. http://www.telegraph.co.uk/news/worldnews/europe/russia/12103602/America-to-investigate-Russian-meddling-in-EU.html.

Gaddis, John Lewis. 2005. *Strategies of containment [electronic resource] : a critical appraisal of American national security policy during the Cold War*. Rev. and expanded ed. New York : Oxford University Press.

Galeotti, Mark. 2015. "The west is too paranoid about Russia's information war'." Guardian, Last Modified July 7 Accessed Feb 8. http://www.theguardian.com/world/2015/jul/07/russia-propaganda-europe-america.

George, Alexander. 1991. *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*. Washington, D.C.: United States Institute of Peace Press.

Goffman, Erving. 1975. *Frame analysis : an essay on the organization of experience*. Harmondsworth: Penguin.

Jackson, Jasper. 2015. "RT sanctioned by Ofcom over series of misleading and biased articles." Guardian, Last Modified Sept 21 Accessed Feb 15. http://www.theguardian.com/media/2015/sep/21/rt-sanctioned-over-series-of-misleading-articles-by-media-watchdog.

James, Josh. 2015. "Data Never Sleeps 3.0." Accessed Jan 15. https://www.domo.com/blog/2015/08/data-never-sleeps-3-0/.

Joes, Anthony James. 1996. *Guerrilla warfare : a historical, biographical, and bibliographical sourcebook*. Westport, Conn; : Westport, Conn.

Kennan, George F. 1946. "861.00/2 - 2246: Telegram; The Charge in the Soviet Union (Kennan) to the Secretary of State." Last Modified Feb 22 Accessed Jan 15. http://nsarchive.gwu.edu/coldwar/documents/episode-1/kennan.htm.

Kennedy, Paula, and Simona Kralova. 2015. "Russian bid for Czech hearts and minds." BBC, Last Modified April 2 Accessed Feb 8. http://www.bbc.co.uk/news/world-europe-32070184.

Lasswell, Harold D. 1927. "The Theory of Political Propaganda." *American Political Science Review* 21 (03):627-631.

Machiavelli, Niccolò. 2005. *The Prince*. Edited by Peter E. Bondanella. Oxford: Oxford University Press.

Marlin, R. 2002. *Propaganda and the Ethics of Persuasion*: Broadview Press.

Mccuen, John J. 2008. "Hybrid Wars." *Military Review*:107-113.

Miskimmon, A., O'Loughlin, B. and Roselle, L. (2014) *Strategic Narratives: Communication Power and the New World Order*. Routledge

Mogherini (2015) Answer given by Vice-President Mogherini on behalf of the Commission (P-013637-15. 3 December 2015). Retrieved from http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2015-013637&language=EN

Nimmo, Ben. 2016. "Propaganda in a New Orbit." Center for European Policy Analysis, Last Modified Jan Accessed Feb 17. http://www.cepa.org/sites/default/files/Info%20War%20Two.pdf.

Nye, Joseph S. 2004. *Soft power: the means to success in world politics*. 1st ed. New York: Public Affairs.

Orenstein, Mitchell A. 2014. "Putin's Western Allies: Why Europe's Far Right Is on the Kremlin's Side." *Foreign Affairs* 25.

Pitas, Ioannis. 2015. *Graph-Based Social Media Analysis*. Boca Raton, Fl, US: Chapman and Hall/CRC.

Pomerantsev, Peter, and Michael Weiss. 2014. *The menace of unreality : how the Kremlin weaponizes information, culture and money*. New York, NY: Institute of Modern Russia.

Rettman, Andrew. 2015. "EU drafts plan on Russia's media 'misuse'." EUObserver, Last Modified June 23 Accessed Feb 16. https://euobserver.com/foreign/129247.

RT (2015) There's something strange in the neighborhood: StratCom East's ghostly targets. RT (13 November 2015). Retrieved from https://www.rt.com/op-edge/321848-rt-west-media-propaganda/

Schelling, Thomas C. 1966. *Arms and Influence*. New Haven: Yale University Press

Silverman, David (2006) Interpreting Qualitative Data (third edition). London: Sage Publica-tions, Inc

Snegovaya, Maria. 2015. "Putin's information warfare in Ukraine: soviet origins of Russia's hybrid warfare." he Institute for the Study of War, Last Modified Sept Accessed Feb 8. http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf.

Sputnik (2015a) Vucic: Serbien fick trea i betyg på grund av Ryssland. Sputnik, 13 November 2015. Retrieved from: http://se.sputniknews.com/asikt/20151113/825158/vucic-serbien-eu-ryssland.html#ixzz3xgcuxydd

Sputnik (2015b) Vučić: Serbien har fået "dårlig karakter" på grund af Rusland. Sputnik, 13 November 2015. Retrieved from: http://dk.sputniknews.com/politik/20151113/435602/vucic-serbien-karakter-rusland.html#ixzz3xgce4wHF

Sputnikbig.ru (2015) 'Reports from the militia of New Russia'. http://sputnikbig.ru/novorossiya/item/6082-svodki-ot-opolcheniya-novorossii-11-11-2015Spruds, Andris, Anda Rožukalne, Klavs Sedlenieks, Martins Daugulis, Diana Potjomkina, Beatrix Tölgyesi, and Ilvija Bruge. 2015. "Internet Trolling as a hybrid warfare tool: the case of Latvia." NATO STRATCOM Accessed 2016. http://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0.

The Economist. 2015. "In the Kremlin's pocket." Last Modified Feb 14 Accessed Feb 2. http://www.economist.com/news/briefing/21643222-who-backs-putin-and-why-kremlins-pocket.

Thomas, Timothy. 2004. "Russia's Reflexive Control Theory and the Military." *The Journal of Slavic Military Studies* 17 (2):237-256. doi: 10.1080/13518040490450529.

Ventre, Daniel. 2011. *Cyberwar and information warfare*. London; Hoboken, NJ: John Wiley.

X. 1947. "The Sources of Soviet Conduct." *Foreign Affairs* 25 (4):566-582. doi: 10.2307/20030065.